REMARKS

In the Official Action mailed 02 April 2008, the Examiner reviewed claims 1-75. The Examiner has rejected claims 1-17, 22-43 and 47-75 under 35 U.S.C. §102(e); and has objected to claims 18-21, 43-46 and 68-71.

Applicant has amended claims 6, 9, 11-14, 22, 25, 31, 33, 34, 36-39, 47, 50, 56, 58, 61-64, 72 and 75, and canceled claims 1-5, 10, 15, 17-21, 23, 24, 26-30, 35, 40, 42-46, 48, 49, 51-55, 60, 65, 67-71, 73 and 74. New claims 76-78 are presented in replacement for claims 1, 26 and 51, respectively. Claims 6-9, 11-14, 16, 22, 25, 31-34, 36-39, 41, 47, 50, 56-59, 61-64, 66, 72, 75-78 are now pending.

Applicant has also amended the specification to correct typographical errors noticed by Applicant upon review of the application, and to add serial numbers of related applications which were not available at the time the application was filed.

Each objection and rejection is respectfully traversed below.

Rejection of Claims 1-17, 22-43 and 47-75 under 35 U.S.C. §102(e)

The Examiner has rejected claims 1-17, 22-43 and 47-75 under 35 U.S.C. §102(e) as being anticipated by Cuccia *et al.* (US 6,151,676). Reconsideration is respectfully requested. There is no algorithm described in Cuccia *et al.* for distribution of a symmetric key as recited in the claims of the present application.

Claims 1, 26 and 51 are canceled in favor of new claims 76-78. Claims 76-78 are parallel method, apparatus and article of manufacture claims. Claims 2-5, 10, 15, 17, 23, 24, 27-30, 35, 40, 42, 43, 48, 49, 52-55, 60, 65, 67-71, 73 and 74 are also canceled. Amendments are made to the balance of the claims as a consequence. The new independent claims are supported by the claims and specification as originally filed. See, Fig. 2, Fig. 3, Figs. 8A-8B for example.

The Examiner's attention is drawn to the claims in related U.S. Application No. 10/653,503 (pending) and U.S. Application No. 10/653,500 (Now U.S. Patent No. 7,299,356).

Reconsideration of the rejection is requested in light of the amendments. Independent claim 77 consolidates selected subject matter from original claims 1-5 and 15, which are now canceled. All of these claims were rejected by the Examiner using the same citation to Cuccia *et al.* So, the rejection is addressed on the merits.

First, for avoidance of doubt, it is not clear to Applicant whether the Examiner is reading the claim term "symmetric encryption key" on the random numbers distributed in the Cuccia *et al.* algorithm. So, Applicant emphasizes that Cuccia *et al.* does not use the random numbers as symmetric keys. The random numbers are used in a process for forming digital signatures which is quite different from the claimed protocol for creating and securely distributing symmetric keys. See, Cuccia *et al.*, Fig. 2, and column 8, line 37 to column 9, line 62. In Cuccia *et al.* the system requires prior distribution of the symmetric key Kpass.

Cuccia *et al.* does rely upon a symmetric key in its algorithm that is created and distributed in a completely different manner than required by the claims herein. Specifically, the "user identifying key" or "Kpass" is used as a symmetric key in Cuccia *et al.* Cuccia *et al.* requires a server having resources for producing the symmetric key in "an extremely secure way" requiring presence of the user "at secure equipment". See, Cuccia *et al.*, column 6, line 50 to column 7, line 15. The "user identifying key" is produced independently at the user machine in a similar fashion. See, Cuccia *et al.*, column 7, lines 19-31. Cuccia *et al.* also mentions that it is known to use a symmetric key in combination with the PKI in the El Gamal algorithm at column 2, lines 62-67.

The algorithm for distribution of the random numbers in Cuccia *et al.* on which the Examiner apparently relies as teaching the claimed process, is not similar to the plurality of exchanges recited in the claims. So, even assuming that the random numbers of Cuccia *et al.* might be used as symmetric keys, they are not distributed in a protocol similar to that claimed herein. In Cuccia *et al.*, all the random numbers are sent in a single package, encrypted using the PKI infrastructure and the Kpass symmetric key. See, Cuccia *et al.*, column 8, lines 37-59. Therefore, it can be seen that the random numbers of Cuccia *et al.* are not symmetric encryption keys as required in claim 1, and are not distributed in a manner similar to the process recited in claim 1.

The Office Action refers to four passages in the Summary of the Invention section of Cuccia *et al.* (column 3, lines 1-53; column 4, lines 3-30; column 4, lines 60-65; column 5, lines 20-27), as corresponding to the limitations of all the rejected claims. The citations are not explained and no difference in the citation is found for any of the dependent claims. Comments on the four cited passages are provided here, showing that they do not support the rejection of these claims.

The passage at column 3, lines 1-53 does not mention a symmetric key. It describes the distribution of "secret fresh random numbers" using a PKI infrastructure.

The passage at column 4, lines 3-30 describes the use of a symmetric key to encrypt the private key used in the algorithm for distribution of the "secret fresh random numbers". The symmetric key, corresponding to "Kpass" mentioned above, is described as "determined from identifying information of the user". However, there is no discussion in this passage of how the symmetric key is distributed to both sides of the communication.

The passage at column 4, lines 60-65, describes the manner in which "user identifying information" can be gathered. The "user identifying information" is used in Cuccia *et al.* to produce the symmetric key (e.g. Kpass). However, this passage proves the point above, that the symmetric key in Cuccia *et al.* is provided in a completely different manner than the protocol recited in the present claims.

The passage at column 5, lines 20-27, describes the storage of the private keys and the symmetric keys ("keys determined from respective user identifying information") for each user at the server. Again, this passage is not relevant to the problem solved by the present invention. Specifically, there is no discussion in this passage, or in any of the four cited passages, of a technique for creating and distributing symmetric keys as required by the present claims.

As mentioned above, in Cuccia *et al.*, the symmetric key (Kpass) is not distributed by an exchange of messages as required by the present claims. Rather, Cuccia *et al.* teaches that the server and the client machine must have secure equipment to produce identical values for the symmetric key. The present invention provides a completely different approach to symmetric key distribution.

As to the dependent claims, the Office Action simply copies the citation to the four cited passages discussed above. Applicant objects to this approach by the Examiner. It will be seen on review of the discussion above, that the cited passages are irrelevant to the dependent claims.

The present invention as stated in the independent claims 76-78, provides a combination of features unlike the prior art. It includes a process for producing session random symmetric encryption keys (SRKi in the specification) and subordinated sub-arrays of data random symmetric keys (DRKi in the specification) that support a plurality of communication sessions and that is scalable for large scale implementation. No similar process is described in Cuccia *et al.* It provides for exchanges of messages using the data random symmetric keys, based on an

iterative exchange as stated in the claims. No similar step is described in Cuccia *et al*. It includes a feature that involves veiling data random symmetric keys in a conversion array using the shared secrets. Again, no similar process is provided in the art. As each of these features is missing from the prior art, the combination is clearly patentable over the art of record.

As stated in the specification, the invention accomplishes both mutual authentication and distribution of a symmetric encryption key in a combined protocol, without preset encryption keys or the PKI infrastructure.

Allowable Subject Matter

Objection to Claims 18-21, 43-46 and 68-71

The Examiner has objected to claims 18-21, 43-46 and 68-71 as being dependent upon a rejected base claim. Such claims are canceled, without prejudice, as mentioned above.

CONCLUSION

It is respectfully submitted that this application is now in condition for allowance, and such action is requested.

The Commissioner is hereby authorized to charge any fee determined to be due in connection with this communication, or credit any overpayment, to our Deposit Account No. 50-0869 (AIDT 1004-1).

Respectfully submitted,

Dated: 31 July 2008

/Mark A. Haynes/

Mark A. Haynes, Reg. No. 30,846

HAYNES BEFFEL & WOLFELD LLP
P.O. Box 366
Half Moon Bay, CA 94019
(650) 712-0340 phone
(650) 712-0263 fax